9/482725

```
SHOW FILE;DS
File   9:Business & Industry(R) Jul/1994-2005/Nov 04
         (c) 2005  The Gale Group
File  13:BAMP 2005/Oct W5
         (c) 2005  The Gale Group
File  15:ABI/Inform(R) 1971-2005/Nov 07
         (c) 2005 ProQuest Info&Learning
File  16:Gale Group PROMT(R) 1990-2005/Nov 08
         (c) 2005 The Gale Group
File  18:Gale Group F&S Index(R) 1988-2005/Nov 07
         (c) 2005 The Gale Group
File  20:Dialog Global Reporter 1997-2005/Nov 08
         (c) 2005 Dialog
File  73:EMBASE 1974-2005/Nov 08
         (c) 2005 Elsevier Science B.V.
File  75:TGG Management Contents(R) 86-2005/Oct W5
         (c) 2005 The Gale Group
File  80:TGG Aerospace/Def.Mkts(R) 1982-2005/Nov 07
         (c) 2005 The Gale Group
File 112:UBM Industry News 1998-2004/Jan 27
         (c) 2004 United Business Media
File 194:FBODaily 1982/Dec-2005/Aug
         (c) format only 2005 Dialog
File 256:TecInfoSource 82-2005/Jan
         (c) 2005 Info.Sources Inc
File 264:DIALOG Defense Newsletters 1989-2005/Nov 07
         (c) 2005 Dialog
File 267:Finance & Banking Newsletters 2005/Nov 01
         (c) 2005 Dialog
File 275:Gale Group Computer DB(TM) 1983-2005/Nov 07
         (c) 2005 The Gale Group
File 387:The Denver Post 1994-2005/Nov 07
         (c) 2005 Denver Post
File 427:Fort Worth Star-Telegram 1993-2004/Feb 25
         (c) 2004 Fort Worth Papers
File 433:Charleston Newspapers 1997-2005/Nov 07
         (c) 2005 Charleston Newspapers
File 485:Accounting & Tax DB 1971-2005/Oct W4
         (c) 2005 ProQuest Info&Learning
File 536:(GARY) POST-TRIBUNE 1992-1999/Dec 30
         (c) 2000 POST-TRIBUNE
File 563:Key Note Market Res. 1986-2001/Aug 03
         (c) 2001 ICC Online Info. Group
File 608:KR/T Bus.News. 1992-2005/Nov 08
         (c)2005 Knight Ridder/Tribune Bus News
File 619:Asia Intelligence Wire 1995-2005/Nov 07
         (c) 2005 Fin. Times Ltd
File 621:Gale Group New Prod.Annou.(R) 1985-2005/Nov 08
         (c) 2005 The Gale Group
File 623:Business Week 1985-2005/Nov 03
         (c) 2005 The McGraw-Hill Companies Inc
File 634:San Jose Mercury  Jun 1985-2005/Nov 07
         (c) 2005 San Jose Mercury News
File 635:Business Dateline(R) 1985-2005/Nov 05
         (c) 2005 ProQuest Info&Learning
File 636:Gale Group Newsletter DB(TM) 1987-2005/Nov 08
         (c) 2005 The Gale Group
File 647:CMP Computer Fulltext 1988-2005/Oct W5
         (c) 2005 CMP Media, LLC
File 660:Federal News Service 1991-2002/Jul 02
```

```
         (c) 2002 Federal News Service
File 674:Computer News Fulltext 1989-2005/Oct W2
         (c) 2005 IDG Communications
File 696:DIALOG Telecom. Newsletters 1995-2005/Nov 07
         (c) 2005 Dialog
File 703:USA Today 1989-2005/Nov 07
         (c) 2005 USA Today
File 710:Times/Sun.Times(London) Jun 1988-2005/Nov 07
         (c) 2005 Times Newspapers
File 727:Canadian Newspapers 1990-2005/Nov 08
         (c) 2005 Southam Inc.
File 728:Asia/Pac News 1994-2005/Nov W1
         (c) 2005 Dialog
File 738:(Allentown) The Morning Call 1990-2005/Nov 06
         (c) 2005 Morning Call

Set     Items   Description
S1        208   (ENCRYPT? (S) (DECRYPT? (2N) KEY? ) (S)  (PUBLIC? (2W)  KE-
             Y?) ) AND PD<=990327
S2        187   RD (unique items)
S3        133   (ENCRYPT? (7N) (DECRYPT? (2N) KEY? ) (S)  (PUBLIC? (2W)  K-
             EY?) ) AND PD<=990327
S4         57   S3 AND (ENCRYPT? (7N) (DECRYPT? (2N) KEY? ) (5W)  (PUBLIC?
             (2W)  KEY?) ) AND PD<=990327
reviewed
S5         49   RD (unique items)
```

```
S (ENCRYPT? (S) DECRYPT? (S) (PUBLIC? (W) KEY?)) AND PD<=990327

Your SELECT statement is:
   S (ENCRYPT? (S) DECRYPT? (S) (PUBLIC? (W) KEY?)) AND PD<=990327

           Items   File
           -----   ----
>>>File 9 processing for PD=  : PD=990327
>>>    started at PD=871119 stopped at PD=990324
              45      9: Business & Industry(R)_Jul/1994-2005/Nov 04
              45     13: BAMP_2005/Oct W5
>>>File 15 processing for PD=  : PD=990327
>>>File 15:     started at PD=710000 stopped at PD=930106
              26     15: ABI/Inform(R)_1971-2005/Nov 07
>>>File 16 processing for PD=  : PD=990327
>>>File 16:     started at PD=19900101 stopped at PD=19950623
              43     16: Gale Group PROMT(R)_1990-2005/Nov 08
>>>File 18 processing for PD=  : PD=990327
>>>File 18:     started at PD=19860423 stopped at PD=19931110
               4     18: Gale Group F&S Index(R)_1988-2005/Nov 07
Processing
>>>File 20 processing for KEY? stopped at KEYTRAK
              33     20: Dialog Global Reporter_1997-2005/Nov 08
               1     73: EMBASE_1974-2005/Nov 08
               9     75: TGG Management Contents(R)_86-2005/Oct W5
>>>File 80 processing for PD=  : PD=990327
>>>File 80:     started at PD=19820101 stopped at PD=19871019
               1     80: TGG Aerospace/Def.Mkts(R)_1982-2005/Nov 07
               1    112: UBM Industry News_1998-2004/Jan 27
       Examined  50 files
>>>File 194 processing for PD=  : PD=990327
>>>File 194:     started at PD=820913 stopped at PD=900601
               1    194: FBODaily_1982/Dec-2005/Aug
               1    256: TecInfoSource_82-2005/Jan
               3    264: DIALOG Defense Newsletters_1989-2005/Nov 07
               5    267: Finance & Banking Newsletters_2005/Nov 01
>>>File 275 processing for PD=  : PD=990327
>>>File 275:     started at PD=140103 stopped at PD=881206
              17    275: Gale Group Computer DB(TM)_1983-2005/Nov 07
               2    387: The Denver Post_1994-2005/Nov 07
       Examined 100 files
               1    427: Fort Worth Star-Telegram_1993-2004/Feb 25
               1    433: Charleston Newspapers_1997-2005/Nov 07
>>>File 485 processing for PD=  : PD=990327
>>>File 485:     started at PD=130000 stopped at PD=920201
               1    485: Accounting & Tax DB_1971-2005/Oct W4
       Examined 150 files
>>>File 536 processing for PD=  : PD=990327
>>>File 536:     started at PD=920101 stopped at PD=970708
               1    536: (GARY) POST-TRIBUNE_1992-1999/Dec 30
               2    541: SEC Online(TM) Annual Repts_1997/Sep W3
               2    542: SEC Online(TM) 10-K Reports_1997/Sep W3
               1    563: Key Note Market Res._1986-2001/Aug 03
       Examined 200 files
>>>File 608 processing for PD=  : PD=990327
>>>File 608:     started at PD=108 stopped at PD=970110
               1    608: KR/T Bus.News._1992-2005/Nov 08
              16    619: Asia Intelligence Wire_1995-2005/Nov 07
>>>File 621 processing for PD=  : PD=990327
>>>File 621:     started at PD=00000000 stopped at PD=19910208
```

```
                1   621: Gale Group New Prod.Annou.(R)_1985-2005/Nov 08
                2   623: Business Week_1985-2005/Nov 03
>>>File 634 processing for PD=  : PD=990327
>>>File 634:     started at PD=12/7/04 stopped at PD=901208
                1   634: San Jose Mercury_ Jun 1985-2005/Nov 07
>>>File 635 processing for PD=  : PD=990327
>>>File 635:     started at PD=1190 stopped at PD=910826
                1   635: Business Dateline(R)_1985-2005/Nov 05
>>>File 636 processing for PD=  : PD=990327
>>>File 636:     started at PD=19880101 stopped at PD=19940323
               19   636: Gale Group Newsletter DB(TM)_1987-2005/Nov 08
       Examined 250 files
               76   647: CMP  Computer Fulltext_1988-2005/Oct W5
>>>File 660 processing for PD=  : PD=990327
>>>File 660:     started at PD=901001 stopped at PD=960721
                4   660: Federal News Service_1991-2002/Jul 02
                5   674: Computer News Fulltext_1989-2005/Oct W2
               21   696: DIALOG Telecom. Newsletters_1995-2005/Nov 07
>>>File 703 processing for PD=  : PD=990327
>>>File 703:     started at PD=880531 stopped at PD=951205
                1   703: USA Today_1989-2005/Nov 07
>>>File 710 processing for PD=  : PD=990327
>>>File 710:     started at PD=880601 stopped at PD=931205
                1   710: Times/Sun.Times(London)_Jun 1988-2005/Nov 07
       Examined 300 files
>>>File 727 processing for PD=  : PD=990327
>>>File 727:     started at PD=107280 stopped at PD=950521
                2   727: Canadian Newspapers_1990-2005/Nov 08
>>>File 728 processing for PD=  : PD=990327
>>>File 728:     started at PD=1022 stopped at PD=970622
                5   728: Asia/Pac News_1994-2005/Nov W1
>>>File 738 processing for PD=  : PD=990327
>>>File 738:     started at PD=900101 stopped at PD=950627
                2   738: (Allentown) The Morning Call_1990-2005/Nov 06
>>>File 742 processing for PD=  : PD=990327
>>>File 742:     started at PD=11 stopped at PD=951021
                1   742: (Madison)Cap.Tim/Wi.St.J_1990-2005/Nov 05
                1   744: (Biloxi) Sun Herald_1995-2005/Nov 03
               22   761: Datamonitor Market Res._1992-2005/Oct
                6   763: Freedonia Market Res._1990-2005/Oct
                8   764: BCC Market Research_1989-2005/Oct
               29   765: Frost & Sullivan_1992-1999/Apr
                3   766: (R)Kalorama Info Market Res._1993-2000/Aug
       Examined 350 files
>>>File 781 processing for PD=  : PD=990327
>>>File 781:     started at PD=830806 stopped at PD=980814
               12   781: ProQuest Newsstand_1998-2005/Nov 08
                1   861: UPI News_1996-1999/May 27

   48 files have one or more items; file list includes 371 files.
   One or more terms were invalid in 211 files.
```

5/3,KWIC/1 (Item 1 from file: 9)
DIALOG(R)File 9:Business & Industry(R)
(c) 2005 The Gale Group. All rts. reserv.

A 01312093 Supplier Number: 23960336 (USE FORMAT 7 OR 9 FOR FULLTEXT)
Candle's MQSecure Brings Web Security To IBM's MOM
(Candle released MQSecure, add-on aimed at bolstering security for IBM's MQSeries messaging-oriented middleware environment)
Newsbytes News Network, p N/A
July 11, 1997
DOCUMENT TYPE: Journal (United States)
LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 1259

(USE FORMAT 7 OR 9 FOR FULLTEXT)

TEXT:
...user who has sent a message cannot deny having sent the message." For authentication, MQSecure encrypts messages with the private key and conducts decryption with the public key .

But MQSecure, he asserted, is also able to address privacy concerns along the lines of...

...are encrypted with a DES (Data Encryption Standard)-like symmetric key. The symmetric key is encrypted with the public key and then decrypted with the private key.

As a result, even if an online thief was able to...

5/3,KWIC/2 (Item 2 from file: 9)
DIALOG(R)File 9:Business & Industry(R)
(c) 2005 The Gale Group. All rts. reserv.

A 01247769 Supplier Number: 23878194 (USE FORMAT 7 OR 9 FOR FULLTEXT)
E-commerce Predicted To Boom In 2 Years In Philippines 04/29/97
(Local Internet presence provider Infinite Information Inc wants to spur the growth of electronic commerce)
Newsbytes News Network, p N/A
April 29, 1997
DOCUMENT TYPE: Journal (United States)
LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 665

(USE FORMAT 7 OR 9 FOR FULLTEXT)

TEXT:
...IP addresses. Meanwhile PGP (Pretty Good Privacy) ensures that the customer order information will be encrypted using the Internet Commerce server's public key , to be decrypted by Infinite's client company using its private key.

As the exclusive local reseller of...

5/3,KWIC/3 (Item 3 from file: 9)
DIALOG(R)File 9:Business & Industry(R)
(c) 2005 The Gale Group. All rts. reserv.

A

```
01235815  Supplier Number: 23866833
 Bankard Set To Intro Virtual Shopping In Philippines
 (Bankard to launch the Virtual Mall that will allow Bankard credit card
 holders with access to the Internet to order products online from the
 convenience of their homes)
Newsbytes News Network, p N/A
April 16, 1997
DOCUMENT TYPE: Journal  (United States)
LANGUAGE: English  RECORD TYPE: Fulltext
WORD COUNT:  670

TEXT:
...works using Secure Socket Layer (SSL) technology, combining encryption
with third-party authentication using a  public   key  and a private key
encryption . The browser will use the  public   key  to  decrypt  the
private  key , or digital ID supplied by Verisign, to verify the
information contained inside. Only  the digital...

...digital ID of Bankard's Internet Commerce server, a secure and encrypted
channel is created.  Public   key -private  key  encryption prevents third
parties or hackers from "listening in" to sensitive information, as they do
...


  5/3,KWIC/4      (Item 4 from file: 9)
DIALOG(R)File   9:Business & Industry(R)
(c) 2005  The Gale Group. All rts. reserv.
```

A

```
00864754  Supplier Number: 23399840    (USE FORMAT 7 OR 9 FOR FULLTEXT)
 S-A UNVEILS SECURITY SYSTEM
 (Scientific-Atlanta Inc has unveiled its digital set-top security system)
Multichannel News, v 18, n 3, p 45+
January 15, 1996
DOCUMENT TYPE: Journal  ISSN: 0276-8593  (United States)
LANGUAGE: English  RECORD TYPE: Fulltext
WORD COUNT:  1146

    (USE FORMAT 7 OR 9 FOR FULLTEXT)

TEXT:
...altogether, or directly link to the Internet from the set-top," he said.

With the  public   key  system, which also uses a private key in a
different way, messages sent in either direction are  encrypted  using the
receiver's  public   key  and  decrypted  by the receiver's private key,
which is embedded in inaccessible storage at the receiver...


  5/3,KWIC/5      (Item 5 from file: 9)
DIALOG(R)File   9:Business & Industry(R)
(c) 2005  The Gale Group. All rts. reserv.

00618375  Supplier Number: 23173801    (USE FORMAT 7 OR 9 FOR FULLTEXT)
 POSTAL SERVICE ANNOUNCES PLAN TO PUT POSTMARKS ON ELECTRONIC MAIL
 (US Postal Service to put postmarks on electronic mail through use of
 digital keys thereby extending legal protection of traditional mail)
San Jose Mercury News , p N/A
April 09, 1995
DOCUMENT TYPE: Regional Newspaper  (United States)
LANGUAGE: English  RECORD TYPE: Fulltext
```

WORD COUNT: 500

(USE FORMAT 7 OR 9 FOR FULLTEXT)

ABSTRACT:
...of individuals' "public keys," long strings of numbers generated by a mathematical algorithm. Any message encrypted with an individual's easily available public key can be decrypted only with their closely held "private key." ...

TEXT:
...sure the supposed sender is authentic. The post office would maintain a directory of individuals' " public keys ," long strings of numbers generated by a mathematical algorithm. Any message encrypted with an individual's easily available public key can be decrypted only with their closely held "private key."

Such a system can be used to apply...

5/3,KWIC/6 (Item 6 from file: 9)
DIALOG(R)File 9:Business & Industry(R)
(c) 2005 The Gale Group. All rts. reserv.

00585728 Supplier Number: 23076269 (USE FORMAT 7 OR 9 FOR FULLTEXT)
Suppliers cashing in on the Internet
(With 800 vendors on line and 5 to 10 signing on every day, security of commercial transactions is becoming an issue on the Internet)
CommunicationsWeek International, n 134, p 36+
November 14, 1994
DOCUMENT TYPE: Journal ISSN: 1042-6086 (United Kingdom)
LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 783

(USE FORMAT 7 OR 9 FOR FULLTEXT)

TEXT:
...encryption and one for decryption. To execute a transaction, each of the parties generates an encryption and a decryption key . The encryption key -- the public key -- is made available in a public file.

The decryption key, however, is kept secret. When...

5/3,KWIC/7 (Item 7 from file: 9)
DIALOG(R)File 9:Business & Industry(R)
(c) 2005 The Gale Group. All rts. reserv.

00564878 Supplier Number: 23069194 (USE FORMAT 7 OR 9 FOR FULLTEXT)
A Privacy Advocate Draws The Blinds On Big Brother; Phil Zimermann's PGP Package Preempts The National Security Agency's Bid To Control Public-Key Cryptography
(Phil Zimmerman's PGP public-key-encryption package has preempted the National Security Agency's bid to control public-key cryptography)
Open Systems Today, n 162, p 56
October 31, 1994
DOCUMENT TYPE: Journal ISSN: 1061-0839 (United States)
LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 2103

A

(USE FORMAT 7 OR 9 FOR FULLTEXT)

TEXT:
...interface, a CompuServe WinCIM interface, and other interfaces built on top of PGP.

COMPLEMENTARY KEYS

Public - key cryptography was invented in 1976, when Whitfield Diffie and Martin Hellman at Stanford University proposed an algorithm that used two keys: a public key to encrypt a message, and a private key to decrypt the message. Their algorithm ensures that the private key cannot be derived from the public key .

The keys are generated in such a way that deriving the secret key from the public key...

...and decryption processes are inverses of each other-you can use the private key to encrypt and then the public key to decrypt . What makes the key public is the fact that it is published. (See Figure 1...

5/3,KWIC/8 (Item 1 from file: 13)

A

DIALOG(R)File 13:BAMP
(c) 2005 The Gale Group. All rts. reserv.

00588764 Supplier Number: 24369349 (USE FORMAT 7 OR 9 FOR FULLTEXT)
Reaching Out to Physicians
(PhyCor (Nashville, TN) turned to Internet to simplify data collection, dissemination)
Article Author(s): Chin, Tyler L
Health Data Management, v 6, n 9, p 36,38,40
September 1998
DOCUMENT TYPE: Journal ISSN: 1069-5699 (United States)
LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 1903

(USE FORMAT 7 OR 9 FOR FULLTEXT)

TEXT:
...based on public key infrastructure technology from Entrust Technologies, Ottawa, Canada.

Public key encryption

A public key encryption infrastructure is a security framework established for generating, distributing, managing, and revoking encryption keys and digital certificates used in encrypting information. In public key encryption, two different keys are generated--one for the sender and one for receivers. What is encrypted with the private key can only be decrypted with the public key , and vice versa. In other words, the key used for decryption cannot be used for encryption as well. Senders give private keys to no one, but give public keys to anyone with whom they want to communicate.

So, PhyCor-affiliated physicians would use their private keys to encrypt data. The recipient of the encrypted data would use the physicians' individual public keys to decrypt it.

When a physician transmits data over the Internet to PhyCor Online's central server...

A

5/3,KWIC/9 (Item 2 from file: 13)
DIALOG(R)File 13:BAMP
(c) 2005 The Gale Group. All rts. reserv.

00578864 Supplier Number: 24260842 (USE FORMAT 7 OR 9 FOR FULLTEXT)
Smartcards: The Intelligent Way To Security
(Obviating the need to remember passwords, smartcards are expected to enable simpler, more secure networking for users)
Article Author(s): Backman, Dan
Network Computing, v 9, n 9, p 168-171
May 15, 1998
DOCUMENT TYPE: Journal ISSN: 1046-4468 (United States)
LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 1723

(USE FORMAT 7 OR 9 FOR FULLTEXT)

TEXT:
...decrypting an S/MIME message, the encrypted session key is downloaded to the card for decryption . Since public key encryption is a very processor-intensive operation, most file encryption is done using conventional symmetric key...

A

5/3,KWIC/10 (Item 3 from file: 13)
DIALOG(R)File 13:BAMP
(c) 2005 The Gale Group. All rts. reserv.

00566976 Supplier Number: 24132249 (USE FORMAT 7 OR 9 FOR FULLTEXT)
How Secure Is Your Computer System?
(According to the IT division of the AICPA, computer/information security will be the number one technology affecting the accounting profession in 1997; employees represent about 70% to 80% of security problem)
Article Author(s): Stevens, Michael G, CPA, JD, LLM
Practical Accountant, v 31, n 1, p 24-32
January 1998
DOCUMENT TYPE: Journal ISSN: 0032-6321 (United States)
LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 5086

(USE FORMAT 7 OR 9 FOR FULLTEXT)

TEXT:
...key is a measure of how secure the encryption is."

photo omitted

Newman noted that public key encryption schemes can not only encrypt a message for privacy, but can also provide a...
...the sender and that the message could not be forged or changed along the way. Public key cryptography can be used for either or both functions. "When I send a message, I encrypt the message using the recipient's public key . They then decrypt it using their private key and their password. Digital signatures can be appended to a...

...based on both the message content and the sender's keys. Using the sender's public key , the message can be authenticated," said Newman.

```
Morris noted that, "a digital signature is a...
?
```

5/3,KWIC/11 (Item 4 from file: 13)
DIALOG(R)File 13:BAMP

A+

00528101 Supplier Number: 23726723 (USE FORMAT 7 OR 9 FOR FULLTEXT)
THE NEW NETWORK: Planning and Protecting Intranet Electronic Commerce
(The article discusses in detail how to provide a secure environment for electronic commerce through the use of an extended intranet)
Information Week, n 608, p 15SUN+
December 02, 1996
DOCUMENT TYPE: Journal ISSN: 8750-6874 (United States)
LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 2608

(USE FORMAT 7 OR 9 FOR FULLTEXT)

TEXT:
...to overall security policies. Private key encryption, such as DES, uses the same key to encrypt and decrypt data. Public key encryption uses one key to encrypt data, and a second key to decrypt data. One of the keys is public without compromising the security of either the second...

...Most encryption products such as SunScreen and ISV solutions for Solaris use a combination of public and private key encryption.
The SunScreen product family is built on SKIP, Simple Key management for IP, SKIP...

5/3,KWIC/12 (Item 5 from file: 13)
DIALOG(R)File 13:BAMP

A

00517627 Supplier Number: 23658458 (USE FORMAT 7 OR 9 FOR FULLTEXT)
Secure Trading on the Net
(The Internet's potential for electronic commerce means that security is a major issue that goes beyond S-HTTP and SSL mechanisms. Included must be security of credit verification and sales processing)
Article Author(s): Kopeikin, Roy
Telecommunications International Edition, v 30, n 10, p 89-94
October 1996
DOCUMENT TYPE: Journal ISSN: 0278-4831 (United States)
LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 2941

(USE FORMAT 7 OR 9 FOR FULLTEXT)

TEXT:
...a special code, typically based upon modular arithmetic or prime numbers, used to initiate an encrypting or decrypting algorithm.
Public key encryption usually involves one such key, where as RSA, a dominant public key method involves two keys, one being secret, and GSM technology involves three unique keys for...
...in mobile phone calls. In the case of SSL protocols for Internet EC, a single public key of the interacting Web-server is transmitted with encrypted data and is also needed to...

5/3,KWIC/13 (Item 6 from file: 13)
DIALOG(R)File 13:BAMP

A

00516921 Supplier Number: 23705494 (USE FORMAT 7 OR 9 FOR FULLTEXT)
Debating Encryption Privacy Vs. Electronic Piracy
(As the demand for individual and corporate electronic privacy increases, it will be matched by packet pirates and government policies to cripple information security)
Article Author(s): Frezza, Bill
Network Computing, v 7, n 18, p 35-36
November 15, 1996
DOCUMENT TYPE: Journal ISSN: 1046-4468 (United States)
LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 1465

(USE FORMAT 7 OR 9 FOR FULLTEXT)

TEXT:
...s Cryptography" (www.rsa.com).

There are two major classes of cryptographic systems: symmetric and public key . In symmetric systems, both the sender and receiver hold the same secret key, with which the sender encrypts data and the receiver decrypts . In public - key systems, keys come in matched pairs. Any sender can use a public key to encrypt data while only the recipient holds the secret portion of the key pair...

...to crack codes grows exponentially as key lengths increase, while the processing time required for public - key encryption and decryption grows at a much slower geometric rate. Even if supercomputers double in power every 18...

5/3,KWIC/14 (Item 7 from file: 13)
DIALOG(R)File 13:BAMP

00512291 Supplier Number: 23640369 (USE FORMAT 7 OR 9 FOR FULLTEXT)
WEB SERVER: SECURITY LOCKDOWN (Part 2 of 4 parts)
(Using secure protocols, with encryption prevents the interception of data and information, by someone between the browser and the server)
Article Author(s): Lee, Michael
Network Computing, v 7, n 14, p 79-80,84+
September 15, 1996
DOCUMENT TYPE: Journal; Guideline ISSN: 1046-4468 (United States)
LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 1334

(USE FORMAT 7 OR 9 FOR FULLTEXT)

TEXT:
...to transmit data, a public-private key pair or a combination of the two.

Data encrypted with a public key can be decrypted only with the corresponding private key, and vice versa. If Alice wants to send Bob a secret message, Alice can use Bob's public key to encrypt the message and then send it to him. Bob can use his private...
...key, he can be assured that no one else reads the message. Only the private key can decrypt the data that was encrypted using the public key .

A

Shared- key algorithms are faster, but it's difficult to ensure that the keys will be exchanged...

5/3,KWIC/15 (Item 1 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)
(c) 2005 ProQuest Info&Learning. All rts. reserv.

00273939 85-14373
Data Security Products: What's Available?
Johnston, R. E.
Infosystems v32n4 PP: 38, 40 Apr 1985
ISSN: 0364-5533 JRNL CODE: BAU

...ABSTRACT: these products are subject to export regulations imposed by the US Department of State. With public - key systems, the key used for encryption can be made public ; only the key used for decryption necessitates security measures. With private-key or single-key systems, one key is used for both encryption and decryption , and good key management is required to ensure confidentiality. Before purchasing any data security software, individual needs should...
850000

A

5/3,KWIC/16 (Item 2 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)
(c) 2005 ProQuest Info&Learning. All rts. reserv.

00197522 83-09083
Data Encryption: Unscrambling the Mystery
Pollock, Harvey
Canadian Datasystems v15n2 PP: 41-42 Feb 1983
ISSN: 0008-3364 JRNL CODE: CAD

...ABSTRACT: of combinations. Racal-Milgo uses the conventional method in conjunction with an adaptation of the public key method in its Datacryptor II. A public key is used for encryption and a private key for decryption . Both conventional and public key management methods in this cryptographic application are sound, reliable, and flexible for present and future...
830000

A

5/3,KWIC/17 (Item 1 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2005 The Gale Group. All rts. reserv.

03816282 Supplier Number: 45447048 (USE FORMAT 7 FOR FULLTEXT)
Protecting Your Privacy
Network Computing, p146
April 1, 1995
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 1171

... However, in 1976, Whitfield Diffie and Martin Hellman suggested a different approach, which they called public key , or asymmetric, cryptography. Here, each key actually consists of two parts - an encryption half (the ' public key ') and a decryption half (the 'private key,' which unlocks data encrypted with the matching public key).

This system allows a more convenient key distribution method - anyone who wishes to communicate with...

19950401

A

5/3,KWIC/18 (Item 2 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2005 The Gale Group. All rts. reserv.

03790501 Supplier Number: 45397059 (USE FORMAT 7 FOR FULLTEXT)
Firepower in the War Against Data Piracy
CommunicationsWeek, p1
March 13, 1995
Language: English Record Type: Fulltext
Document Type: Newsletter; Trade
Word Count: 923

... Standard. The complication is how to get the key - securely - to the other party.

The public key encryption method uses two sets of numbers or keys, related by a mathematical function. One key encrypts the message and the second key decrypts it.

Typically, each user posts his or her public key and makes it available to...

...sender use the public key for encrypting messages, while each message recipient has a private key that can decrypt ecrypted messages.

RSA has licensed public - key encryption technology to a number of vendors, including Apple Computer Inc., Lotus Development Corp. and Novell ...

19950313

A

5/3,KWIC/19 (Item 3 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2005 The Gale Group. All rts. reserv.

03230976 Supplier Number: 44437097 (USE FORMAT 7 FOR FULLTEXT)
Clipper opponents gird for encryption fight
Electronic Engineering Times, p4
Feb 14, 1994
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 627

... alternatives to Clipper but that any such alternatives 'must preserve the law-enforcement element.'

In public - key encryption, end-user encryption keys are openly published to enable anyone to send encrypted data...

...who then decrypt the material with a private key. The NSA reportedly has difficulty in decrypting public - key - encrypted messages.

The Clipper endorsement contains three flaws, according to a policy paper released last month...

19940214

5/3,KWIC/20 (Item 4 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

A

02696313   Supplier Number: 43600536

RSA public-key encryption plan wins support

Computerworld, p34
Jan 25, 1993
Language: English   Record Type: Abstract
Document Type: Magazine/Journal; Tabloid; Trade

ABSTRACT:

RSA Data Security's public - key data encryption standard is winning the endorsements of an increasing number of vendors. At a...

...workgroup software. Resulting from the efforts of three MIT mathematicians, RSA's standard employs a public - key design. It uses two keys--one public and one private. Information encrypted with the public key can be decrypted only with the private key. The use of two keys also yields a 'digital signature...

19930125

?

5/3,KWIC/21 (Item 5 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2005 The Gale Group. All rts. reserv.

A+

02103190 Supplier Number: 42725268 (USE FORMAT 7 FOR FULLTEXT)
Next step is encryption: DATA SECURITY MAY BE BUNDLED WITH NEXT'S OPERATING SYSTEM
Electronic Engineering Times, p18
Feb 3, 1992
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 549

... one of its chief scientists, Richard Crandall.

The system is based on a technology called public key encryption. Public key systems use a matched pair of mathematically related encryption - decryption keys : a public key and a secret key. Each key performs a one-way transformation of data. Public keys are listed in a directory, but secret keys are known only to their owners. For example, to send a private message, user A encrypts a message with user B's public key . User B decodes the message with his secret key.

Public key systems also can be...
19920203

A+

5/3,KWIC/22 (Item 6 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2005 The Gale Group. All rts. reserv.

01702732 Supplier Number: 42122495 (USE FORMAT 7 FOR FULLTEXT)
Network-Based Authentication: The Key to Security
Network Computing, p98
June, 1991
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 2545

... is stored someplace on the network, accessible to all other users.

To encrypt something, the public key is used; messages are then decrypted using private keys . Anybody can encrypt a message using the public key , but the only way to read it is with a private key. Public and private keys are the inverse of each other: anything encrypted with one can only be decrypted with the other. A message encrypted with a public key cannot be decrypted with the same key; a similar limitation applies to private keys.

The value of public...
19910601

A

5/3,KWIC/23 (Item 1 from file: 20)
DIALOG(R)File 20:Dialog Global Reporter
(c) 2005 Dialog. All rts. reserv.

04374559 (USE FORMAT 7 OR 9 FOR FULLTEXT)
OnLine: How security was breached: Computing and the Net
GUARDIAN
February 11, 1999
JOURNAL CODE: FGDN LANGUAGE: English RECORD TYPE: FULLTEXT
WORD COUNT: 351

... public key and a private key which are related by a mathematical factoring problem. Messages encrypted using the public key can be decrypted only by someone with the private key.
The only way (or so it was thought...

19990211

A

5/3,KWIC/24 (Item 2 from file: 20)
DIALOG(R)File 20:Dialog Global Reporter
(c) 2005 Dialog. All rts. reserv.

04061465 (USE FORMAT 7 OR 9 FOR FULLTEXT)
VLSI TECHNOLOGY: VLSI partners with 3Com to provide data security from the desktop to the network
M2 PRESSWIRE
January 19, 1999
JOURNAL CODE: WMPR LANGUAGE: English RECORD TYPE: FULLTEXT
WORD COUNT: 565

(USE FORMAT 7 OR 9 FOR FULLTEXT)

... integrates a number of VLSI's data security on-chip building blocks covering functionality for encryption and decryption , hashing, public - key acceleration and random number generation. 3Com products using the chip will deliver unimpeded throughput for...

19990119

A

5/3,KWIC/25 (Item 3 from file: 20)
DIALOG(R)File 20:Dialog Global Reporter
(c) 2005 Dialog. All rts. reserv.

04039987 (USE FORMAT 7 OR 9 FOR FULLTEXT)
VLSI Partners With 3Com to Provide Data Security From the Desktop to the Network
BUSINESS WIRE
January 18, 1999
JOURNAL CODE: WBWE LANGUAGE: English RECORD TYPE: FULLTEXT
WORD COUNT: 679

(USE FORMAT 7 OR 9 FOR FULLTEXT)

... integrates a number of VLSI's data security on-chip building blocks covering functionality for encryption and decryption , hashing, public - key acceleration and random number generation. 3Com products using the chip will deliver unimpeded throughput for...

19990118

X

5/3,KWIC/26 (Item 4 from file: 20)
DIALOG(R)File 20:Dialog Global Reporter
(c) 2005 Dialog. All rts. reserv.

01869129 (USE FORMAT 7 OR 9 FOR FULLTEXT)
The encryption factor
ELECTRONICS TIMES, pPage 24
June 01, 1998

JOURNAL CODE: FETS LANGUAGE: English RECORD TYPE: FULLTEXT
WORD COUNT: 1346

(USE FORMAT 7 OR 9 FOR FULLTEXT)

... security associated with public keys.
Another way to avoid the time delay associated with the encryption and decryption of public key ciphers is to speed up the encryption /decryption processes using a crypto accelerator. One company specialising in this sort of device is...

19980601

5/3,KWIC/27 (Item 5 from file: 20)
DIALOG(R)File 20:Dialog Global Reporter
(c) 2005 Dialog. All rts. reserv.

A
01821727 (USE FORMAT 7 OR 9 FOR FULLTEXT)
The encryption factor
Stewart Gore
ELECTRONICS TIMES, pPage 24
June 01, 1998
JOURNAL CODE: FETS LANGUAGE: English RECORD TYPE: FULLTEXT
WORD COUNT: 1343

(USE FORMAT 7 OR 9 FOR FULLTEXT)

... security associated with public keys.
Another way to avoid the time delay associated with the encryption and decryption of public key ciphers is to speed up the encryption /decryption processes using a crypto accelerator. One company specialising in this sort of device is...

19980601

5/3,KWIC/28 (Item 1 from file: 75)
DIALOG(R)File 75:TGG Management Contents(R)
(c) 2005 The Gale Group. All rts. reserv.

A
00211568 SUPPLIER NUMBER: 20822788 (USE FORMAT 7 FOR FULL TEXT)
The role of public key cryptography, digital signatures, and digital certificates in electronic commerce.
Schutzer, Daniel
The Journal of Lending & Credit Risk Management, v80, n10, p24(4)
June, 1998
ISSN: 0021-986X LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 2435 LINE COUNT: 00204

... documents.
To communicate in private, a message should be encrypted with the other party's public key . When information in someone's public key is encrypted, that person is the only one who can read the message, as it requires his or her private key to decrypt the message. Using public /private keys to encrypt a message, however, is much more inefficient (requires a lot more processing steps and longer...

...difficult for two parties to remotely exchange a symmetric key in secret. For this reason, public key pairs are only used to securely exchange a shared secret key, a session key. The session is then encrypted using the session key. Note that only one party's public key needs to be known to exchange a secure session key. Some alternative approaches that do not even require knowledge of a party's public key can be used for symmetric key exchange.

A party digitally signs an electronic document by...

19980600

A

5/3,KWIC/29 (Item 1 from file: 194)
DIALOG(R)File 194:FBODaily
(c) format only 2005 Dialog. All rts. reserv.

1992191
PUBLIC KEY ALGORITHM CHIP PROTOTYPE
Contact Lt David Blocker, 315/330-2203, Contr Specialist; Lt Douglas Atkinson, 315/330-3241, Program Manager. Duration: 24 Months. Design, fabricate, test and del an experimental model (a hardware chip set) from an existing Govt furnished algorithm. The algorithm performs a Public Key encryption and decryption function using error correction codes. The hardware chip set may eventually be used for key encryption techniques in communications security. The algorithm will first be studied and implemented in software according to MIL-STD-2167A. This software will encode and decode data with the ability to monitor the algorithm's operation. The architecture for the hardware chip set will be extracted and optimized for reliable and fast operation. A small No. of chip sets will be produced for experimental purposes and to determine some actual performance capabilities of the algorithm. Requirements for performance of the contr include experience in the ADA programming language, experience in hardware chip production, and expertise in encryption/decryption and error correction algorithms (familiarity with Goppa codes will be particularly helpful). Classification of the contr is at the Secret level. See Notes 11, 49 and 68. For purposes of Note 11, the small business size standard for this acquisition is 1,000 persons. Closing date for submission of responses is twenty days from date of pub of this notice. Respondees are requested to provide their Commercial and Govt Entity (CAGE) No. and Reference No. B-8-3526-L in their submission. (103)

SPONSOR: Rome Air Development Center, Griffiss AFB, NY 13441-5700
PUBLICATION DATE: APRIL 14, 1988
ISSUE: PSA-9569

... model (a hardware chip set) from an existing Govt furnished algorithm. The algorithm performs a Public Key encryption and decryption function using error correction codes. The hardware chip set may eventually be used for key...

A

5/3,KWIC/30 (Item 1 from file: 536)
DIALOG(R)File 536:(GARY) POST-TRIBUNE
(c) 2000 POST-TRIBUNE. All rts. reserv.

08114002 (USE FORMAT 7 OR 9 FOR FULLTEXT)
POSTAL SERVICE PREPARES TO POSTMARK E-MAIL SOON
David Bank, Knight-Ridder Writer
Post-Tribune (Gary IN), ALL ED, P D16
Monday, April 24, 1995
LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT SECTION HEADING: OTM
Word Count: 445

```
  (USE FORMAT 7 OR 9 FOR FULLTEXT)

...sure the supposed sender is authentic. The post office would maintain a
directory of individuals' " public  keys ," long strings of numbers
generated by a mathematical algorithm. Any message  encrypted  with an
individual's easily available  public  key  can be  decrypted  only with
their closely held "private key."

    Such a system can be used to apply...


  5/3,KWIC/31     (Item 1 from file: 608)
DIALOG(R)File 608:KR/T Bus.News.
(c)2005 Knight Ridder/Tribune Bus News. All rts. reserv.
```

A

```
00269784          Story Number:  6820    (USE FORMAT 7 OR 9 FOR FULLTEXT)
 POSTAL SERVICE ANNOUNCES PLAN TO PUT POSTMARKS ON ELECTRONIC MAIL
David Bank
San Jose Mercury News
April 9, 1995  22:48 E.T.
DOCUMENT TYPE: Newspaper    RECORD TYPE: Fulltext    LANGUAGE: English
WORD COUNT:    550

...TEXT:  sure the supposed sender is authentic. The post office would
maintain a
directory of individuals' " public  keys ," long strings of numbers
generated by
a mathematical algorithm. Any message  encrypted  with an individual's
easily
available  public  key  can be  decrypted  only with their closely held
"private
key."
      Such a system can be used to apply...


  5/3,KWIC/32     (Item 1 from file: 619)
```

A

```
DIALOG(R)File 619:Asia Intelligence Wire
(c) 2005 Fin. Times Ltd. All rts. reserv.

05056924 HJWELAAAAIW  (USE FORMAT 7 FOR FULLTEXT)
 INTERNET BANKING INVITING VIRTUAL HOLDUPS?
DATAQUEST (India)
Tuesday, September 30, 1997
JOURNAL CODE:  DQST  LANGUAGE:  English  RECORD TYPE:  Fulltext
WORD COUNT: 1,152

EXPANDED PUBLICATION DATE:   19970930

...an underlying exchange of
goods, thus raising barriers to virtual holdups.

Basics Of Digital IDs

 Public  key  encrypting is a technique which uses a pair of keys instead
of a
single key for encrypting the message, which has to be transmitted. The
keys, called the  public /private  key  pair, are a matched set assigned to
every user. Each key of the pair performs...
```

...one-way transformation on the data and has inverse functions, i.e. what one key encrypts , only the other can decrypt . The public key is available to everyone, while the private key is only for the owner. Encrypting can...

5/3,KWIC/33 (Item 2 from file: 619)
DIALOG(R)File 619:Asia Intelligence Wire
(c) 2005 Fin. Times Ltd. All rts. reserv.

A+

05010091 HIVC6AB0AIW (USE FORMAT 7 FOR FULLTEXT)
THE KEY TO KEYS
DATAQUEST (India)
Sunday, August 31, 1997
JOURNAL CODE: DQST LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 2,317

EXPANDED PUBLICATION DATE: 19970831

...were sent he would have to try to break all of them.

Public Key Encryption

Public key encryption is one of the most radical developments in the field of cryptology. Originally conceived by a group at MIT, public key encryption provides a completely new way of looking at the key distribution problem. Until the invention of this technique, cryptologists always assumed that both the encryption and decryption keys have to be kept secret to guarantee security. Public key encryption questions this basic assumption. The basic premises of the public key encryption are:

* Each user possesses two keys E and D. E is to be used...E(D(P))=P

Given that these two conditions hold and the fact that all encryption keys are public and decryption keys private then digital signatures can be achieved by using the following procedure-if A has to transmit a message to B, he first decrypts the plaintext using his own private decryption key . He then proceeds to encrypt this message using B's public key . The message is now sent to B. B first decrypts the message using his private decryption key , after which he encrypts the result using A's public encryption key . The final result is the original plaintext. The entire procedure is displayed in the figure...

5/3,KWIC/34 (Item 1 from file: 647)
DIALOG(R)File 647:CMP Computer Fulltext
(c) 2005 CMP Media, LLC. All rts. reserv.

01161946 CMP ACCESSION NUMBER: NWC19980515S0030

A

Smartcards: The Intelligent Way To Security
Dan Backman
NETWORK COMPUTING, 1998, n 909, PG168
PUBLICATION DATE: 980515

JOURNAL CODE: NWC   LANGUAGE: English
RECORD TYPE: Fulltext
SECTION HEADING: Workshops
WORD COUNT: 1766

PUBLICATION DATE: 980515
... decrypting an S/MIME message, the encrypted session key is downloaded to the card for decryption . Since public key encryption is a very processor-intensive operation, most file encryption is done using conventional symmetric key...

5/3,KWIC/35   (Item 2 from file: 647)
DIALOG(R)File 647:CMP Computer Fulltext
A (c) 2005 CMP Media, LLC. All rts. reserv.

01111191   CMP ACCESSION NUMBER: NWC19961115S0016
Debating Encryption Privacy Vs. Electronic Piracy (FreeWire)
Bill Frezza
NETWORK COMPUTING, 1996, n 718, PG35
PUBLICATION DATE: 961115
JOURNAL CODE: NWC   LANGUAGE: English
RECORD TYPE: Fulltext
SECTION HEADING: Columnists
WORD COUNT: 1484

PUBLICATION DATE: 961115
... s Cryptography" (www.rsa.com)
There are two major classes of cryptographic systems: symmetric and public key . In symmetric systems, both the sender and receiver hold the same secret key, with which the sender encrypts data and the receiver decrypts . In public - key systems, keys come in matched pairs. Any sender can use a public key to encrypt data while only the recipient holds the secret portion of the key pair...

...to crack codes grows exponentially as key lengths increase, while the processing time required for public - key encryption and decryption grows at a much slower geometric rate. Even if supercomputers double in power every 18...
?